IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of: Vandergeest et al.	Examiner: Thomas M. Ho
Application No.: 09/747,770	Group Art Unit: 2132
Filed: December 22, 2000	Our File No.: 10500.00.8171
For: METHOD AND APPARATUS FOR PROVIDING USER AUTHENTICATION	Docket No.: 0500.0008171

APPEAL BRIEF PURSUANT TO 37 C.F.R. § 41.37

Dear Sir:

Appellants submit this brief further to the Pre Appeal Brief Request for Review filed March 7, 2006, in the above-identified application.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

Entrust Limited is the real party in interest in this appeal by virtue of an executed Assignment from the named Inventors of their entire interest to Entrust Technologies Limited and an executed name change. The Assignment evincing such ownership interest was recorded on April 12, 2001, in the United States Patent and Trademark Office at Reel 011688, Frame 0001. The Name Change was recorded on October 18, 2006, in the United States Patent and Trademark Office at Reel 018405, Frame 0217.

II. RELATED APPEALS AND INTERFERENCES

To Appellants' knowledge, there are no related Appeals or Interferences filed, pending, or decided.

III. STATUS OF CLAIMS

The originally filed Application contained claims 1-31. Claims 1, 3, 5, 6 and 15 were amended during prosecution of the present application. Claims 1-26 are rejected. Claims 27-31 are allowed. A copy of appealed claims 1-26 and allowed claims 27-31 are attached in Appendix A. Of the pending claims, 1, 6, 10, 17, 21 and 27 are independent.

IV. STATUS OF AMENDMENTS

A Pre Appeal Brief Request for Review was filed on March 7, 2006 in response to the Final Office Action mailed on September 7, 2005 and Advisory Action mailed on January 30, 2006. No amendments were made to the claims, however, subsequent to the Final Office Action. The claims listed in Appendix A reflect the claims as they stood at the time the Final Office Action was mailed.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter is generally directed to a method and apparatus for providing user authentication that employs multi-factor authentication techniques. (Specification page 1, lines 10-13, Specification page 5, lines 18-24). More specifically, a method, in one example, accommodates a user that may use one of a plurality of different destination units. First factor authentication data, such as user identification data and/or password data, is sent by a first unit to another unit, such as an authentication unit that determines which destination unit will receive an authentication code to be used as second factor authentication information to authenticate the user. The authentication code is sent to the determined destination unit and the authentication code is subsequently returned to the authentication unit, such as by the destination unit or through another unit. The user is then considered authenticated when the returned authentication code matches the sent authentication code. (Specification page 5, line 18 through page 6, line 28).

In one embodiment, a primary channel and an alternate channel are used during the same session to provide multifactor user authentication. In addition, one of a number of destination units is selected as the destination unit to facilitate authentication of a user. Among other advantages, an out of band authentication code cannot be intercepted nor are hardware tokens required which are not in communication with a network which can potentially allow an unscrupulous party to gain access to a user's device. (Specification page 3, line 38 through page 4, line 28). In one example, a method provides user authentication by communicating primary authentication information, such as user identification data and/or password data to an authentication unit using a primary channel, such as over the Internet. An authentication code is generated by the authentication unit on a per session basis and is sent to a first device or another destination unit via an alternate or secondary channel during the session.

In one example, FIG. 3, submitted with the original filing of the present application and shown below, illustrates an embodiment where a destination unit (e.g., cell phone, pager or other device), other than a first unit is used to receive a generated authentication code from an authentication unit. In this example, both a primary channel and a secondary channel are used during the same session to provide authentication of a user. The first unit 300 communicates over a primary wireless channel 310 with, for example, a second unit such as a web server through a wireless network. (Specification, page 12 through page 18). A destination unit shown as third unit 306 such as a pager or cell phone communicates with the second unit 302 via a wireless back channel 312 such as an SMS (short message service) channel. A generated authentication code, used as a second authentication factor, is generated by the authentication unit 304 for communication via the second or wireless back channel 312 while the primary channel 310 is used to send, for example, first factor authentication information such as a user ID information and/or password information. The authentication code that is provided via the alternate channel 312 (e.g., back channel) is then, for example, displayed on the display of the third unit and a user then enters the displayed authentication code through a user interface on the first unit 300. The entered authentication code is then resent by the first unit 300 to the second unit 312 via the primary channel. The second unit passes the resent authentication code to the authentication unit 304 where the authentication unit compares the resent authentication code with the authentication code that was sent to the third unit. (Specification, page 12, lines 12-30).

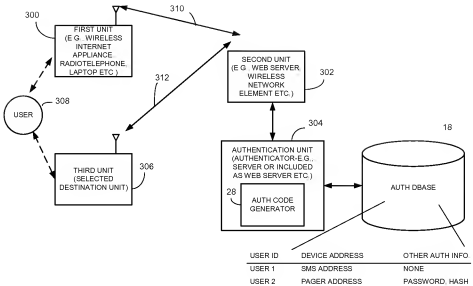

FIG. 3

FIG. 3 Application No. 09/747,770 (Present Application)

FIG. 1 submitted with the original application and shown below shows a first device 10 and an authentication unit 12 wherein authentication information 32 (first factor authentication information) is sent from the first device 10 to the authentication unit 12 based on a request, for example, from the authentication unit 12. The authentication unit 12 determines which unit, in this case unit 10, is a destination unit. The authentication unit 12 sends secondary authentication information (e.g., second factor authentication information) via a back channel during the same session and the secondary authentication information is then resent from the device 10 to the authentication unit 12 (resent secondary authentication information 36). As such, this embodiment shows that the first unit and destination unit are the same unit. In contrast, FIG. 3 shows that a unit other than the first unit (third unit 306) as the unit that receives the secondary authentication information via a back channel. Among other advantages, in one example, a primary secondary channel may be employed and the resending of authentication information is

employed to facilitate multi-factor authentication so that a primary channel and a back channel may be used during the same session to provide user authentication.

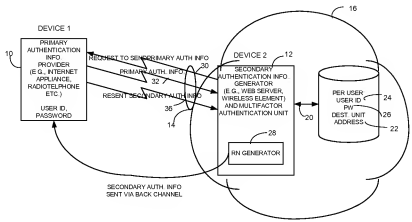

FIG. 1

FIG. 1 Application No. 09/747,770 (Present Application)

A. BRIEF SUMMARY OF THE PRIOR ART REFERENCES - THE CRANE REFERENCE

Only one reference has been used under 35 U.S.C. §103 to reject the unallowed claims. As best understood, U.S. Patent No. 6,510,236 ("Crane") is directed to an authentication framework for managing authentication requests from different types of authentication devices 55 such as different biometric devices, token cards, or other alternative authentication devices. (Column 1, lines 39-57). Crane is directed to enabling clients or servers and Internet based applications to incorporate alternate authentication devices 55 such as token cards or biometric scanners into current authentication schemes. If a client has an authentication device 55 attached to it, Crane determines if the authentication device 55 is one of a plurality of permitted authentication device types. (Column 2, lines 14-28). As such, Crane attempts to allow a user to

use different card readers or types of authentication devices 55 that are already connected in the system through a server. An application server 12 services requests from different application clients 14. The request includes a user ID and device ID identifying a respective client and an authentication device 55 that is attached to the particular client sending the request. As stated in Crane:

> In operation, each given application client passes to the application server a request for authentication. The request includes a user ID and device ID identifying a respective client and an authentication device coupled thereto. The application server (if it trusts the device and has support for it) determines which device authentication server the request is intended, and then routes given authentication data to that server. If the device authentication server verifies that the authentication data [e.g. scanned fingerprint] is acceptable for authentication, an authorization token is returned to the client. (Column 2, lines 29-38).

In Crane, the "authorization token" is not an "authentication code." The authorization token" of Crane confirms that the user is already authenticated based on the authentication data (e.g., fingerprint data) sent in the request.

FIG. 4 of Crane (shown below) and the associated text (column 4, line 42 to column 6, line 14) illustrate in more detail the approach described in Crane. As shown and described, a client unit 14 that utilizes its own authentication device 55 such as a fingerprint scanner is used to scan a user's fingerprint, for example, and sends this "authentication data" along with a user ID and a device ID wherein the device ID indicates the type of authentication device 55 – in this example a type of fingerprint scanner – that was used to create the device data. This data is used by Crane so that Crane's system can determine whether the fingerprint scanner of the particular device is an approved type of scanner since different authentication devices may use different encoding protocols for example (column 4, lines 40-47). Crane is not directed to utilizing a destination device as a mechanism for authenticating and sending an authentication code that is used to authenticate a user.

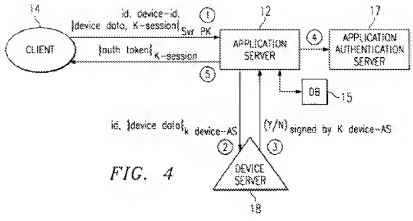

FIG. 4

FIG. 4 U.S. Patent No. 6,510,236 (Crane et al.)

The application server 12 of Crane does not perform an authentication function with respect to the data (column 4, lines 66-67) but instead determines whether the authentication device type, such as the type of fingerprint scanner used by client 14, is supported by the framework. (Column 5, lines 1-13). In particular, each fingerprint scanner or authentication device is registered with the framework and stored in database 15 by its device id. The application server 12 scans the local database 15 to determine if the authentication device connected with client 14 is of a registered type. If it is a registered type of fingerprint scanner, the application server 12 reencrypts the device data with the key and the user ID and provides this string of information to a device authentication server 18. The device authentication server 18 then performs user authentication by verifying the authentication data and provides a simple "yes or no" response back to the application server 12. (Column 5, lines 14-37). The "yes or no" response is then processed by the application server 12 which then knows the user is to be given access. It may then pass an "authorization token" – not an authorization code – back to the user preferably encrypted in the session key. The authorization token may be obtained from the

application authentication server 17 in one example. The authorization token is sent to the client to let the client know that the user is has been authenticated as a legitimate user. Crane is directed to a different method and system from that claimed by Applicants. Crane, among other differences with Applicants' claimed invention, uses the "authorization token" merely to notify the client that the user has been "authorized", e.g., the finger print has been confirmed, and that access has been granted for the user.

As stated in Crane, its framework:

> includes an application server that manages authentication request traffic from a variety of clients having disparate authentication devices or schemes. The application server manages such request traffic or without having to verify specific authentication device data which typically varies depending upon the device type and vendor. (Column 6, lines 6-12).

The "authorization token" or "authentication token" described in Crane is a token either generated by the application server 12 or obtained from the application authentication server 17 by the application server 12. These "tokens" indicate or serve as confirmation data indicating that results of the user authentication process.(Col. 5, lns 28-43). The Crane system sends the "authorization token" or "authentication token" back to the client <u>after</u> the user is authenticated by the device authentication server 18 or the application authentication server 17. Crane states:

> <u>Upon receipt</u> [of a yes or no confirmation that the user is authentic], the application server processes the responses as required and, <u>as a result, knows the user is to be given access. It may then</u> pass an authorization token back to the user, preferably encrypted in the session key…(Column 5, lines 33-37).
>
> <u>After the user is authorized by the application authentication server</u>, the authentication token is returned to the client, preferably encrypted in the session key. This completes the processing period. (emphasis added) (Column 5, lines 39-43).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-4 and 6-26 stand rejected under 35 U.S.C. §103(a) in view of Crane et al. (U.S. Patent No. 6,510,236). Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Crane et al. (U.S. Patent No. 6,510,236) and Bellare et al. (U.S. Patent No. 5,673,318).

VII. ARGUMENT

The obviousness rejection directed to claims 1-4 and 6-26 must be reversed because it fails to provide a prima facia case of obviousness. For example, the reference does not teach what is alleged. In addition, the rejection fails to provide support for where the cited reference allegedly teaches the claimed subject matter. Also, the motivation to modify Crane is not supported since Crane does not disclose the modification as alleged in the office action.

The obviousness rejection as to claim 5 must also be reversed based on at least similar grounds as to claim 1.

A. THE OBVIOUS REJECTION MUST BE REVERSED SINCE THE CRANE REFERENCE DOES NOT TEACH THE CLAIMED SUBJECT MATTER AS ALLEGED

During prosecution, the Patent and Trademark Office bears the initial burden of providing a *prima facia* case of obviousness. *In re: Glaug*, 283 F.3d. 1335, 1338, 62 USPQ 2d. 1151, 1152 (Fed. Cir. 2002). The factual considerations relevant to the legal determination of obviousness addresses the scope and content of the prior art. *Graham v. John Deere*, 383 US1, 148 USPQ 459 (1966). In addition, "the prior art reference (or references when combined) must teach or suggest all the claim limitations." (Manual of Patent Examining Procedure, Section 706 (20.2(J)), page 700-48 citing *In re: Vaeck*, 947 F.2d. 488, 20 USPQ 2d. 1438 (Fed. Cir. 1991)). Accordingly, if the reference does not teach what is alleged in the rejection, the claims cannot be rejected as unpatentable.

a. CLAIMS 1, 2, 17 AND 18

Claim 1 reads:

> A method for providing user authentication comprising:

(a) sending, by a first unit [APPLICATION SERVER 12], user identification data to an authentication unit [DEVICE AUTHENTICATION SERVER 18];

(b) using, user identification data, sent by the first unit [APPLICATION SERVER 12] to determine which destination unit [APPLICATION AUTHENTICATION SERVER 17] will receive an authentication code to be used to authenticate the user;

(c) sending the authentication code to the determined destination unit [APPLICATION AUTHENTICATION SERVER 17] based on the user identification data;

(d) returning the authentication code to the authentication unit [DEVICE AUTHENTICATION SERVER 18]; and

(e) authenticating the user when the returned authentication code matches the sent authentication code.(emphasis added and alleged corresponding elements from the Crane reference).

The Office Action states that the Crane reference teaches basically the entire claim. The Office Action equates the application server 12 of Crane to the "first unit," the application authentication server 17 of Crane to the "destination unit" and the authentication device server 18 of Crane to the claimed "authentication unit" (final action pg. 5). The above claim has been edited to show in brackets the corresponding structure from Crane as alleged in the final office action. As seen from the claim language, it appears that the office action confuses terms and that the terms do not equate to the actual claim terms.

For example, the final office action states as to clause (b) in claim 1:

> "Using the user identification data sent by the first unit to determine which destination unit will receive the authentication code to authenticate the user, where the user identification data is used by the Application Server (Item 12) to access a database (Item 15) to determine which destination unit (which particular [application] authentication server [17]) will receive the authentication code to authenticate the user, and wherein the user identification data sent by the first unit

> the Application server is used as part of the authentication process both to determine the device type and to select the application server [12]. (Column 5, lines 1-20) et seq." (Final Office Action, page 5). (emphasis added).

First the rejection equates the "destination unit" with the application authentication server 17 of Crane. As claimed then, Crane would need to teach that the user identification data ("id") sent by the application server 12 (first unit) is used to determine which application authentication server 17 (destination unit) will receive an authentication code that is later sent to the destination unit and returned and analyzed to see if the returned authentication code matches the sent authentication code. However, no such determination is made in Crane as there in only one application authentication server 17 and no user ID data is described as being used to make such a determination.

The Office Action cites to column 5, lines 1-20, etc. However, the cited portion of column 5 actually refers to the fingerprint authentication device 55 that is connected with the client 14. Applicants respectfully submit that the Office Action mischaracterizes the Crane reference since, inter alia, the user identification data ("id") in Crane is not used to determine which authentication server 17 (alleged to be the claimed destination unit) will receive an authentication code to be used to authenticate the user. There is only one application authentication server 17 and the "id" data in Crane is not shown to be used to determine which authentication server 17 is to receive an authentication code that is used to authenticate the user. In fact, Crane teaches that there may be multiple authentication units – device authentication servers 18 – but not authentication servers 17. As noted in Crane, if multiple device authentication servers 18 are used, then the user ID can be used to route the authentication data from the scanner to the appropriate authentication unit. (col. 2 lines 32-38). There is no teaching of the claimed operation as to a destination unit as alleged in the rejection.

Second, the rejection states that Crane teaches that the user identification data sent by the first unit – the application server 12 – is "used…to select the application server." In other words the user ID data sent by the application server is used to select itself. This does not make sense. The claim does not require such an operation.

Third, there is no identification in the rejection as to what in Crane corresponds to the claimed "authorization code" that is sent to the "determined destination unit" nor does the reference teach the claimed subject matter regarding the authentication code and its communication as claimed. For example as to clause (c) of claim 1, the office action (page 5) cites to Col. 5, lns 23-27 and states:

> sending the authentication code to the determined destination unit based on the user identification data, where the authentication code (code used to authenticate the client) will be sent to the destination unit (the Application authentication server, Item 17), based on user identification data.

The cited portion does not identify what data in Crane corresponds to the authentication code that is sent to a determined destination unit (the application authentication server 17). In fact, the cited portion actually refers *to the device authentication server 18* which is the authentication unit according to the rejection – not the destination unit. (See column 5, line 25). Accordingly, the reference does not teach what is alleged and the claims are in condition for allowance.

Fourth, as to clause (e), the Office Action cites Crane at column 5, lines 33-37 as allegedly teaching "authenticating the user when the returned authentication code matches the sent authentication code". The office action states that "the code is sent back to the user in the form of a token" and hence equates the claimed "authentication code" to the "authorization token" described in Crane. However, the "authorization token" in Crane is not used to "authenticate the user" – user "authentication" has already been completed by the time the

"authorization token" is sent to the client. (col. 5, lns29-37). The "authorization token" in Crane is used as a confirmation message that indicates that the authentication process is complete and that the user is "authorized." As claimed, the "authentication code" is used in the authentication process to determine whether a user is authentic. As claimed, a sent authentication code is checked with a returned authentication code to see if they match, if so the user is determined to be authenticate. The "authentication token" in Crane is not sent, returned or checked to see if a sent "authorization token" matches a returned "authorization token" as required by the claim. The office action cites Column 5, lines 33-37 as allegedly teaching the claimed authentication process using the claimed "authentication code". This portion states:

> Upon receipt, the application server processes the responses as required and, as a result, knows the user is to be given access. It may then pass an authorization token back to the user, preferably encrypted in the session key.

As can be seen, the system already knows that the user is to be given access when the "authorization token" is sent. The authorization token in Crane tells the client that the authentication process is already complete and that the user is authorized. There is no mention that the "tokens" in Crane are used to authenticate a user based upon a returned token that matches a sent token. Also it appears that the "tokens" in Crane are generated after authentication has taken place in Crane. Again, since the reference does not teach what is alleged, Applicants respectfully submit that the rejection must be reversed.

In addition, the office action admits that Crane fails to disclose returning the authentication code to the authentication unit but that it would have been obvious in view of Crane itself to send an authentication code instead of a simple yes/no answer since it is alleged that Crane discloses this modification in his own invention. However, there is no teaching in Crane to authenticate a user based on the authentication codes being sent returned and checked for matches as claimed and as noted above.

The cited portion of the reference, namely column 5, lines 60-64 "that all the message and response string may be returned instead of a digital signature." (see page 6 of response) does not teach what is alleged. Instead, the cited portion merely states that the various messages or response strings may be communicated "over a secure link as opposed to using encryption and digital signature schemes." Accordingly, what Crane actually teaches is that the "yes" or "no" response or the "authentication token" or other information *may instead of being digitally signed, may be sent via a secure link*. It does not teach or suggest the returning of an authentication code that is then matched with a sent authentication code to authenticate a user as required by the claim. Instead it teaches that the existing information used in Crane can be sent in a different manner – using a secure link instead of digital signature schemes. Accordingly, the rejection must be reversed for one or more of the above reasons and the claims should be passed to allowance.

b. CLAIMS 3, 12,19 AND 24

Column 4, line 58 to column 5, line 27 has been cited as allegedly teaching a step of maintaining per user destination unit data that includes at least one destination unit identifier per user and wherein using the user ID data to determine which destination unit will receive the authentication code includes sending the authentication code to the determined destination unit based on the stored per user destination unit identifier, as required in claim 3. As such, the claim allows for a user to have stored on its behalf data representing a destination unit identifier per user. Using the Examiner's logic that the application authentication server 17 corresponds to the claimed "destination unit", the cited portion fails to teach the claimed subject matter. The Office Action states that the "per user destination unit identifier is the device ID." (Final Action, page 7). However, the destination unit is said to be the "authentication server [17]" as to claim 1

(see Final Action, page 5). The device ID in Crane does not refer to the application authentication server 17, but to the contrary actually refers to fingerprint devices 55 that are connected to the client 14. (Column 4, lines 42-63). Accordingly, the reference has been misapprehended and the rejection should be reversed.

c. CLAIMS 4, 13 AND 24

The Office Action cites column 4, line 48 to column 5, line 36 of Crane as allegedly teaching a step of "receiving user input in response to the step of sending the authentication code and waiting to return the authentication code to the authentication unit until receipt of the user input." However, this cited portion cannot be taught by the cited reference because, as to claim 1, the Examiner admitted that "Crane fails to…disclose returning the authentication code to the authentication unit." (Page 6). Accordingly, the cited portion cannot teach "waiting to return the authentication code to the authentication unit until receipt of the user input" because the Examiner admits as to claim 1 that the reference fails to teach or disclose returning the authentication code to the authentication unit in rejection of claim 1. Accordingly, the rejection for this claim should also be reversed.

d. CLAIMS 6, 7, 9, 17 AND 20

These claims have been rejected for the same reasons as claim 1. Accordingly, Applicants respectfully reassert the relevant remarks made above with respect to claim 1. As such, the rejection of this claim should also be reversed. In addition, these claims require using user identification data to determine which destination unit "other than the first unit" will receive an authentication code to be used to authenticate the user. The method also includes sending the authentication code to the determined destination unit based on the user identification data and receiving the returned authentication code back after sending the authentication code. As such,

the user identification data sent by the first unit was used to determine which destination unit other than the first unit will receive the authentication code. This is shown, for example, in FIG. 3 of Applicants' pending application as reproduced above. The rejection makes no mention of, nor has the rejection identified, any teaching in Crane that performs these steps since Crane is silent as to utilizing user identification data to determine which application authentication server 17 will receive an authentication code to be used to authenticate the user (again, applying the rejection's equivalent that the application authentication server 17 has been equated to the claimed destination unit). Also, as noted above, the application authentication server 17 in Crane does not receive an authentication code, it generates the authorization token (which as discussed above is not an "authentication code" as claimed) and provides the authorization token. Moreover, there is no discussion of application authentication servers (alleged destination units) that are identified by user identification data. Accordingly, Applicants respectfully submit that the rejection should be reversed.

e. CLAIM 8

Applicants respectfully reassert the relevant remarks made above with respect to claim 3 and also note that the claim requires that the user identification data is used to determine which destination unit, other than the first unit, will receive the authentication code by sending the authentication code to the determined destination unit based on the stored per user destination unit identifier. Since the reference fails to teach the claimed subject matter, Applicants respectfully submit that the claim rejection should be withdrawn.

f. CLAIMS 10, 11, 15, 16, 21, 22 AND 26

The Office Action rejected claim 10 "for the same reasons" as claim 1. Applicants respectfully submit that the claim language of claim 10 has not been addressed in the office

action since the claim requires, among other things, "primary authentication information," "secondary authentication information" as well as "a primary wireless channel" and that the authentication code is the "secondary authentication information." As such, this claim sets out more detail as to a multi-factor authentication method, which again is not disclosed in Crane. Moreover, the Office Action fails to address the above language as there is absolutely no statement as to what in Crane corresponds to the "secondary authentication information" and the "primary authentication information" as claimed nor the "primary channel".

In addition, the Office Action states that "the additional wireless back [sic] limitation is discussed in claim 15." However, there is no discussion in Crane of using a primary wireless channel and a wireless back channel wherein the authentication code is sent on the wireless back channel to a destination unit and the primary authentication information is sent on the primary wireless channel by a primary authentication information provider as claimed. Referring to the rejection of claim 15, the Office Action cites Column 1, lines 25-39 and Column 6, lines 1-14. However, Applicants are unable to find any mention of communicating or sending authentication codes, used to authenticate a user, on a wireless back channel to a destination unit based on primary authentication information during the same session as required by the claim. To the contrary, the cited portion appears silent as to the use of any wireless primary channel or wireless back channel and the corresponding claim limitations as to the information sent and other operations as claimed. The cited portion merely states that the client server in Crane can use Internet based applications to use alternate authentication devices such as alternate token cards and biometric devices. The cited portion is silent as to the claimed subject matter and as such, the rejection must be reversed.

B. THE COMBINATION OF CRANE AND BELLARE FAILS TO TEACH THE CLAIMED SUBJECT MATTER AND, AS SUCH, CLAIMS 5, 14 AND 25 ARE IN CONDITION FOR ALLOWANCE

Applicants respectfully reassert the relevant remarks made above with respect to claim 1 and, as such, these claims are also in condition for allowance at least for these reasons.

VIII. CONCLUSION

For the reasons advanced above, Appellants submit that the Examiner erred in rejecting pending claims 1-26 and respectfully request reversal of the decision of the Examiner.

Respectfully submitted,

Date: 10-19-06

By: Christopher Reckamp
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P.C.
222 N. LaSalle Street
Chicago, Illinois 60601
PHONE: (312) 609-7599
FAX: (312) 609-5005

CLAIMS ON APPEAL

Claim 1. A method for providing user authentication comprising:

(a) sending, by a first unit, user identification data to an authentication unit;

(b) using, user identification data, sent by the first unit to determine which destination unit will receive an authentication code to be used to authenticate the user;

(c) sending the authentication code to the determined destination unit based on the user identification data;

(d) returning the authentication code to the authentication unit; and

(e) authenticating the user when the returned authentication code matches the sent authentication code.

Claim 2. The method of claim 1 including the step of generating the authentication code on a per authentication session basis and sending the authentication code to the determined destination unit in response to the generated authentication code.

Claim 3. The method of claim 1 including the step of maintaining per user destination unit data including at least one destination unit identifier per user and wherein the step of using the user identification data to determine which destination unit will receive the authentication code includes sending the authentication code to the determined destination unit based on the stored per user destination unit identifier.

APPENDIX A

Claim 4. The method of claim 1 including the step of receiving user input in response to the step of sending the authentication code and waiting to return the authentication code to the authentication unit until receipt of the user input.

Claim 5. The method of claim 1 including the steps of:

prior to returning the authentication code to the authentication unit, digitally signing, by the first unit, the returned authentication code to produce a digitally signed authentication code that was received from the determined destination unit; and

verifying the digitally signed authentication code as part of step (e).

Claim 6. A method for providing user authentication comprising:

receiving, from a first unit, user identification data by an authentication unit;

using the user identification data sent by the first unit to determine which destination unit, other than the first unit, will receive an authentication code to be used to authenticate the user;

sending the authentication code to the determined destination unit based on the user identification data;

receiving a returned authentication code back after sending the authentication code; and

authenticating the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

Claim 7. The method of claim 6 including the step of generating the authentication code on a per authentication session basis and sending the authentication code to the determined destination unit in response to the generated authentication code.

APPENDIX A

Claim 8. The method of claim 6 including the step of maintaining per user destination unit data including at least one destination unit identifier per user and wherein the step of using the user identification data to determine which destination unit, other than the first unit, will receive the authentication code includes sending the authentication code to the determined destination unit based on the stored per user destination unit identifier.

Claim 9. The method of claim 6 wherein the returned authentication code is digitally signed and including the step of verifying, by the authenticating unit, the digitally signed authentication code as part of the step of authenticating the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

Claim 10. A method for providing user authentication comprising:

sending primary authentication information on a primary wireless channel by a primary authentication information provider to an authentication unit during a session;

using the primary authentication information to determine which destination unit will receive an authentication code as secondary authentication information via a wireless back channel to be used to authenticate the user;

sending the authentication code on the wireless back channel to the destination unit based on the primary authentication information during the same session;

returning the authentication code on the wireless primary channel to the authentication unit during the same session; and

authenticating the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel.

Claim 11. The method of claim 10 including the steps of generating and sending the authentication code on a per authentication session basis.

Claim 12. The method of claim 10 including the step of maintaining per user destination unit data including at least one destination unit identifier per user and wherein the step of using the primary authentication information to determine which destination unit will receive the authentication code includes sending the authentication code to the destination unit based on the stored per user destination unit identifier.

Claim 13. The method of claim 10 including the step of receiving user input in response to the step of sending the authentication code and waiting to return the authentication code to the authentication unit until receipt of the user input.

Claim 14. The method of claim 10 including the steps of:

prior to returning the authentication code to the authentication unit, digitally signing, by the first unit, the returned authentication code to produce a digitally signed authentication code that was received from the determined destination unit; and

verifying the digitally signed authentication code as part of authenticating the user.

Claim 15. The method of claim 10 including the step of sending the authentication code on the wireless back channel to the destination unit using at least one of a short message session (SMS) channel, a paging channel and a control channel.

Claim 16. The method of claim 10 including the step of: validating the primary authentication information.

Claim 17. A storage medium comprising:

memory containing executable instructions that when executed by one or more processors, causes the one or more processors to:

receive, from a first unit, user identification data by an authentication unit;

use the user identification data to determine which destination unit, other than the first unit, will receive an authentication code to be used to authenticate the user;

send the authentication code to the determined destination unit based on the user identification data;

receive a returned authentication code back after sending the authentication code; and

authenticate the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

Claim 18. The storage medium of claim 17 including memory containing instructions that when executed by one or more processors, causes the one or more processors to

generate the authentication code on a per authentication session basis and send the authentication code to the determined destination unit in response to the generated authentication code.

Claim 19. The storage medium of claim 17 including memory containing instructions that when executed by one or more processors, causes the one or more processors to maintain per user destination unit data including at least one destination unit identifier per user and send the authentication code to the determined destination unit based on the stored per user destination unit identifier.

Claim 20. The storage medium of claim 17 including memory containing instructions that when executed by one or more processors, causes the one or more processors to digitally sign the returned authentication code and verify, by the authenticating unit, the digitally signed authentication code as part of authenticating the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

Claim 21. A storage medium comprising:

memory containing executable instructions that when executed by one or more processors associated with one or more devices, causes the one or more processors to:

send primary authentication information on a primary wireless channel by a primary authentication information provider to an authentication unit during a session;

use the primary authentication information to determine which destination unit will receive an authentication code as secondary authentication information via a wireless back channel to be used to authenticate the user;

send the authentication code on the wireless back channel to the destination unit based on the primary authentication information during the same session;

return the authentication code on the wireless primary channel to the authentication unit during the same session; and

authenticate the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel.

Claim 22. The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to generate and send the authentication code on a per authentication session basis.

Claim 23. The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to maintain per user destination unit data including at least one destination unit identifier per user and send the authentication code to the destination unit based on the stored per user destination unit identifier.

Claim 24. The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to receive user input in response to the step of sending the authentication code and wait to return the authentication code to the authentication unit until receipt of the user input.

Claim 25. The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to:

prior to returning the authentication code to the authentication unit, digitally signing, by the first unit, the returned authentication code to produce a digitally signed authentication code that was received from the determined destination unit; and

verifying the digitally signed authentication code as part of authenticating the user.

Claim 26. The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to send the authentication code on the wireless back channel to the destination unit using at least one of a short message session (SMS) channel, a paging channel and a control channel.

Claim 27. A system for providing user authentication comprising:

a first unit;

a second unit operatively coupleable to the first unit via a primary wireless channel and operatively coupleable to an authenticator; and

a third unit, operatively coupleable to the second unit via a wireless back channel,

the first unit operative to send primary authentication information via the primary channel during a session to the second unit;

the authenticator operative to use the primary authentication information to determine which destination unit, other than the first unit, will receive an authentication code as secondary authentication information via the wireless back channel and wherein the destination unit is the third unit;

the second unit operative to the send the authentication code on the wireless back channel to the destination unit based on the primary authentication information sent via the primary channel during the same session;

the first unit operative to return the authentication code on the wireless primary channel to the second unit during the same session; and

the authenticator operative to authenticate the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel.

Claim 28. The system of claim 27 wherein the authenticator maintains per user destination unit data including at least one destination unit identifier per user and sends the authentication code to the second unit for transmission to the destination unit based on the stored per user destination unit identifier.

Claim 29. The system of claim 27 wherein the first unit includes an interface to receive user input in response to the sending of the authentication code and wherein the first unit waits to return the authentication code for the authenticator until receipt of the user input.

Claim 30. The system of claim 27 wherein the first unit includes a cryptographic engine and prior to the first unit returning the authentication code for the authenticator, digital signs the returned authentication code to produce a digitally signed authentication code that was received from the third unit; and wherein the authenticator verifies the digitally signed authentication code as part of authenticating the user.

APPENDIX A

Claim 31. The system of claim 27 wherein the second unit send the authentication code on the wireless back channel to the third unit using at least one of: a short message session (SMS) channel, a paging channel and a control channel.

EVIDENCE APPENDIX

[NONE]

RELATED PROCEEDINGS

[NONE]